NETWORK SYSTEM AND METHOD FOR SECURE COMMUNICATION SERVICE

FIELD OF THE INVENTION

The present invention relates to a network system having secure service facility and, more particularly, to a network system including central management and control equipment in center office and a plurality of switching equipment to improve communication confidentiality by the use of encryption keys prepared in encryption section of switching equipment at each time of call establishment.

BACKGROUND OF THE INVENTION

As the network infrastructure for information transfer improves, the importance of security is reviewed and recognized. Today, networks for transferring information are essential for daily life because networks can reduce temporal and spatial restriction either in business or in private life.

However, the way of handling information differs depending on intention of a person who originates the information. Sometimes, messages regarded important by outside people are handled imprudently. In a private network such as an intra-company network, lines leased from telecommunications operating agencies are usually used.

This means the information is transferred through public region. At present, however, adequate measures are not always taken against illegal action such as wiretapping. One reason is that intra-company communications are originally based on

connections between extension lines within a company.

Considering such situation, various encryption technologies for secure communication have been developed to cope with illegal wiretapping, unauthorized alteration etc. to information content to be transferred through a network. An outline of the secure communication is explained in FIG. 8.

In the case of (I) shown in FIG. 8, data to be sent from an originating party T1 to a receiving party T2 is assumed to be kept remained as that in the original message (i.e. plaintext). According to this method, wiretapping or alteration can be easily conducted at T3 on the way of transmission.

On the other hand, in the case of (II) in FIG. 8, data is transmitted after the data has been encrypted using an encryption key (A) at originating party T1. At receiving party T2, the encrypted data is regenerated to the plaintext using a decryption key. Operation of decryption is required to restore the data into plaintext, and either wiretapping or alteration onto the data being transmitted becomes difficult.

With regard to the method of encryption, the following two methods are known. A common-key encryption method in which an encryption key (A) and a decryption key (B) are identical; and a public-key encryption method in which the key (B) differs from the key (A).

The common-key encryption is a method that encryption and decryption are carried out using the same key at originating party T1 and receiving party T2 respectively. The public-key encryption method, represented by the RSA encryption method,

is such that encryption is basically performed using a public key and decryption is performed using a private key, to which a one-way function is applied.

The common-key encryption method is used for encrypting a message itself because high speed processing is possible. On the other hand, the public-key encryption method is not oriented for high speed processing, while it may easily be installed by software. Therefore, the public-key encryption method is mainly applied to key delivery for performing the common-key encryption method.

As for methods of practical encryption by the use of encryption key, the following two methods are known: a block encryption method represented by DES, and a stream encryption method by functioning random number on bit-by-bit basis.

Among examples of present communication systems, a terminal encrypting method and a line encrypting method are known. According to the terminal encrypting method, encryption is performed at each terminal point using security equipment 100 provided in each terminal, as shown in FIG. 9. In the line encrypting method as shown in FIG. 10, security equipment 100 is provided in TDM equipment, and encryption is performed on line-by-line basis.

In the terminal encrypting method in FIG. 9, it is assumed that receiving parties are different call by call. (Apparently, security equipment 100 of the identical design is required for both originating party and receiving party.) After a call is connected, an encryption key (or a decryption key for a receiving

party) is transferred between a pair of security equipment located in each party, using the public-key encryption method. Thus, the public key is shared between the originating party and the receiving party.

On the other hand, in the line encrypting method, encryption is carried out between, for example, TDM (multiplexing) equipment 101 at the unit of guaranteed transmission line (e.g. 1.544 Mbps) as shown in FIG. 10. Such a system is realized by using the stream encryption method, which enables simple and high-speed processing. However, when lines include a cross connect, security equipment 100 is required line-by-line. A key management function is also required.

Current secure systems have been generally realized by combining methods described above. One example is shown in FIG. 11. After a call is connected between a terminal A and a terminal B, a common key for encrypting messages is generated in security equipment 100 at terminal A (step S1). In order to transfer the common key to terminal B, the common key is encrypted using the public key of terminal B and is transmitted (step S2).

Terminal B decrypts received encrypted data using the private key of terminal B itself (step S3). Thus the common key is shared between terminals A and B. Accordingly, using the common key shared between the terminals, messages are encrypted in security equipment 100 at terminal A and the secure communication is started.

Recently, in the field of economic activities related to electronic commerce, the Internet etc., measures for individual

authentication, security and so on have been applied. However, a mechanism to enable secure communication between any of parties at any time and place has not been provided yet. A system is desired to have such facility.

Presently, as mentioned above, security equipment 100 must basically be implemented line by line where secure communication is required. In addition, secure communication between any party is not possible using only security equipment 100 which has already been installed. Secure communication with newly added parties needs to install another security equipment 100 with additional cost.

Further, in order to build security function to the maximum extent, a key management function becomes essential. It is complicated for network users to share keys for performing the aforementioned public-key encryption method. This requires maintaining keys by a unified system. Under such integrated key management, the object to be managed may be restricted.

The present invention provides a network system having a secure service facility to solve above-mentioned problems.

SUMMARY OF THE INVENTION

It is an object of the invention to provide a network system particularly in a private network having secure service facility which may not require users' intervention.

It is a further object of the invention to provide a network system having secure service which can improve confidentiality by applying secure service facility independently for specified

users without system modification.

It is a still further object of the invention to provide a network system having secure service facility wherein central management and control equipment is provided to conduct a unified key management function.

According to the present invention, a network system having secure communication service facility to solve aforementioned problems includes central management and control equipment and a plurality of switching equipment, either of which further includes an encryption section. When a call requesting secure communication is originated, central management and control equipment encrypts in the own encryption section (a) a public key of switching equipment accommodating a called party; and (b) a common key to encrypt a message to be transmitted between the switching equipment related to the message communication. These keys are delivered to the switching equipment having detected an originated call at each time a call requesting secure communication is originated.

According to one aspect of the invention, central management and control equipment maintains public keys of a plurality of switching equipment in a database. Central management and control equipment receives a dial number of a called party and a user identification number from the switching equipment detecting the call. Central management and control equipment then retrieves in the own database (a) a public key of the switching equipment accommodating the called dial number; and (b) a public key of the switching equipment detecting the

originated call. For this purpose, the called dial number and the user identification number assigned in the switching equipment detecting the call are used respectively. Then, central management and control equipment generates a common key from the retrieved public key of the switching equipment accommodating the called party and a public key of the switching equipment detecting the originated call.

According to another aspect of the invention, switching equipment detecting an originated call encrypts a common key received from central management and control equipment using a public key of switching equipment accommodating a called party, to forward to the switching equipment accommodating the called party. Then, the switching equipment accommodating the called party decrypts the encrypted common key using the own private key of the switching equipment.

According to another aspect of the invention, switching equipment detecting an originated call is controlled so as to transit to the secure communication mode each time a call is originated.

According to still another aspect of the invention, switching equipment detecting an originated call is controlled so as to transit to the secure communication mode at the time of detecting information in the call which request to transit to the secure communication mode.

As described above, central management and control equipment in a center office which performs unified key management and operation is individually connected to each of

a plurality of switching equipment through a common channel signaling network. The keys may be delivered at desired time. Key delivery corresponding to each called party on call-by-call basis enables central management and control equipment to manage and control suitable condition for the encryption.

The above and other features of the invention will become apparent in the following description of the embodiments of the invention and the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows the principle of the secure service facility in a network system in accordance with the present invention.

FIG. 2 shows a database provided in central management & control equipment 20 of a center office.

FIG. 3 shows a procedure for key delivery.

FIG. 4 further shows a flow of the aforementioned procedure in switching equipment 10.

FIG. 5 shows an example of the overall system configuration mainly explaining the functional block diagram of the switching equipment in which encryption section 100 is attached.

FIG. 6 shows one embodiment of encryption section 100.

FIG. 7 shows another embodiment of the present invention.

FIG. 8 shows the outline of the secure communication.

FIG. 9 shows the terminal encryption method.

FIG. 10 shows the line encryption method.

FIG. 11 shows an example of the conventional system having secure communication facility.

DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 shows the principle of secure communication facility of the network system in accordance with the present invention. In FIG. 1, a circuit switched public network 22 includes a plurality of switching equipment SW1-SW4.

Subscriber terminals DT are connected to switching equipment SW1-SW4 respectively. Each switching equipment SW1-SW4 is individually connected through a signaling network 21 such as No.7 common channel signaling network to a center office in which unified key management operation is performed.

The center office includes central management & control equipment 20. Each of switching equipment has a security section. Central management & control equipment 20 and each switching equipment constitute a network, which is independent of circuit switched public network 22, enabling to deliver keys at desired time. In FIG. 1, for example, when a call is originated from data terminal DT2, switching equipment SW2 transmits information related to a called party DT1 to central management & control equipment 20.

Then, central management & control equipment 20 retrieves in a database and transmits to switching equipment SW2 a retrieved public key related to the called party and a common-key information. Switching equipment SW2 encrypts the common-key information using the public key related to the called party and transmits the encrypted information to switching equipment SW4 in which the called party is accommodated. Switching

equipment SW4 may obtain the common key by decrypting the received information using the own private key of switching equipment SW4.

Thus, message information may be encrypted and transferred between switching equipment SW2 and SW4 using the common key.

Accordingly, in the present invention, encryption keys may be delivered at any desired time through the individual connection between any of the switching equipment and a center office in which the unified key management operation is performed. This enables not only to integrate key management function that has been performed independently in conventional systems, but also to facilitate key modification when desired for the delivery to related equipment. Thus, enhanced flexibility and expandability to overall network can be obtained.

In addition, using the above-mentioned encryption method on call-by-call basis, secure communication function is carried out at a point within network nodes, as compared to the line encryption method. This makes either illegal wiretapping or alteration to messages difficult. In private networks, switching equipment and subscribers connected to the switching equipment are generally located within the same firm. It is therefore mainly between a plurality of switching equipment that secure communication function is required.

Referring to FIG. 2, a database is provided in central management & control equipment 20 located in a center office. Central management & control equipment 20 provides key

management and modification functions 200 based on database 201. In database 201, public keys and private keys corresponding to each of switching equipment A - X are registered. A public key is used for encrypting data for transmission, which is open to any other switching equipment.

On the other hand, a private key is to be used in switching equipment for decrypting data which has been encrypted and transmitted from other switching equipment. In FIG. 2, public keys and private keys given to the center office are registered in a database 202. The public keys and the private keys are used when information is transferred between the center office, which includes central management & control equipment 20, and each of the switching equipment.

Referring to FIG. 3, a procedure for the key delivery is shown. In FIG. 3, it is assumed for explanation that, in a network which includes a plurality of the switching equipment, a call is originated from a subscriber accommodated in switching equipment 10 to a subscriber accommodated in switching equipment 11.

When a call is originated from a calling party, a communication mode of switching equipment 10 is shifted to the secure communication mode (i.e. the automatic secure communication mode). It may also be possible, however, that a calling party sends a distinctive number corresponding to the secure service prior to an originating number, which causes to shift to the secure communication mode (i.e. the individual secure communication mode).

In the latter case, switching equipment 10 is shifted to the secure service mode when a distinctive number (i.e. a predetermined number assigned to the secure service) is identified from the dialed information.

In FIG. 3, switching equipment 10 having been shifted to the secure service mode encrypts both the dial number of the called party and the user identification number in the switching equipment. This operation is performed using a public key 202 of central management & control equipment 20, which is open throughout the network in advance. It is then transferred to central management & control equipment 20 through No.7 common channel signaling network 21 (step S1).

In central management & control equipment 20, encrypted data transmitted from switching equipment 10 is decrypted using private key 202 of central management & control equipment 20. Thus, the dial number of the called party and the user identification number of switching equipment 10 are recognized.

Then, central management & control equipment 20 obtains the public key (e.g. ***b : refer to database 201) of switching equipment 11 in which the called party's dial number is maintained (i.e. the called party is accommodated) by retrieving in database 201 according to the called dial number. Furthermore, central management & control equipment 20 encrypts, and then transmits, the obtained public key of switching equipment 11 and a common key to be used in switching equipment 10 and 11 (step S2).

Then, switching equipment 10 decrypts the encrypted data

sent from central management & control equipment 20 using the own private key of switching equipment 10. Thus switching equipment 10 can recognize the public key of switching equipment 11 and the common key. Furthermore, switching equipment 10 encrypts the decrypted common key using the public key of switching equipment 11 to transmit to switching equipment 11.

Referring to FIG. 4, the above-mentioned process in switching equipment 10 is explained in more detail. Switching equipment 10, when processing a call request from the subscriber terminal DT, transmits the secure service request together with the dial number of the called party (step S11). This secure service request is detected by call control switch 110 of switching equipment 10 (step S12).

Then, control section 111 performs processing for managing the call, extracting the called party number, deciding applicability of the secure service for the relevant subscriber, preparing a dialogue data to the center office and so on (step S13). The dialogue data prepared in control section 111 is then transmitted through interface 112 to central management & control equipment 20 via common channel signaling network 21 (step S14).

As mentioned above, central management & control equipment 20 decides whether the secure service is allowed for the related terminal using a subscriber data (not shown). Then, also as mentioned above, central management & control equipment 20 performs functions such as key management, retrieval and selection of applicable mode according to database 201 (refer

to FIG. 2) (step S15).

Furthermore, in switching equipment 10, control section 111 requests central management & control equipment 20 to update the encryption keys etc, and also issues a connection start order and secure communication start order to call control switch 110 (step S16). On receipt of the secure communication start order, call control switch 110 connects encryption section 100 with a sending information (step S17).

Encryption section 100 encrypts the sending information connected by call control switch 110 using the public key. Encryption section 100 also has a decryption function to decrypt encrypted information using a private key.

Referring back to FIG. 3, switching equipment 11 decrypts the received encrypted information using the own private key of the switching equipment 11. Thus, the common key may be recognized in switching equipment 11.

At this time, sharing the common key for secure communication has been realized between switching equipment 10 and 11 (more precisely, between encryption sections 100 in each switching equipment). Then, when preparation of the common key is completed in encryption section 100 of switching equipment 11, return information is transmitted back to encryption section 100 of switching equipment 10.

Meanwhile, it may also be possible to send announce message or other special signal to the related terminals in switching equipment 10 and 11 to indicate the secure service process being prepared. After the synchronization is completed between each

encryption section of the relevant switching equipment, the secure message communication is started.

In encryption section 100 of switching equipment 10, encryption is executed using the common key already shared with the encryption section of switching equipment 11. There is provided an encryptor which employs an encryption scheme such as DES, Triple DES etc. in encryption section 100. The encrypted data is then transmitted.

In encryption section 100 of switching equipment 11, the received encrypted data is decrypted using the common key by the reverse procedure of the encryption process in encryption section 100 of switching equipment 10. Then, the decrypted message is forwarded to the terminal accommodated in switching equipment 11. A message originated by a terminal in switching equipment 11 may be processed similarly but in the opposite direction to the above-mentioned procedure.

Referring to FIG. 5, a preferred embodiment of the system configuration is illustrated, where the functional block of switching equipment attached with encryption section 100 is mainly explained. In FIG. 6, a preferred block diagram of encryption section 100 is illustrated. A functional block of switching equipment 10 is explained hereafter referring to FIG. 5, which is common to any of the switching equipment.

Switching equipment 10 includes analogue subscriber circuit 114 and digital subscriber circuit 115. The circuits 114 and 115 are connected to an analogue terminal and a digital terminal respectively according to the class of terminals DT

accommodated to switching equipment 10.

Switching equipment 10 also includes call control switch 110 which further includes switch 110a and signal processing subsystem 110b. In addition, switching equipment 10 has trunk 113 having interface with a circuit switched network 22. Switching processing subsystem 111 includes central processing circuit 120, information translator 121, and common channel signaling circuit 122 connected to common channel signaling network 21.

Overall control is performed by central processing circuit 120 in switching processing subsystem 111 referring to information translator 121. Control signals to/from equipment connected to common channel signaling network 21 are transferred by central processing circuit 120 through the common channel signaling circuit 122.

Supervisory circuit 131 in signal processing subsystem 110b supervises output status of trunk 113 connected to a circuit switched network 22. Switch controller 132 controls route selection function of switch 110a under the control of central processing circuit 120.

D-channel control circuit 130 supervises digital subscriber circuit 115 to decide the D-channel status of a terminal DT. Supervisory circuit 131 supervises analogue subscriber circuit 114 to detect origination of a call. On detecting an originated call, D-channel control circuit 130 and supervisory circuit 131 inform central processing circuit 120 of a called dial number.

As explained later in FIG. 6, central processing circuit 120 encrypts the called dial number and the user identification number of the originating switching equipment in encryption section 100 using the public key of central management & control equipment 20. These encrypted data are then transmitted to central management & control equipment 20 through common channel signaling network 21 via common channel signaling processing circuit 122.

Upon receipt of a common key from central management & control equipment 20, central processing circuit 120 controls switch controller 132 to select a route in switch 110a. The message information encrypted by encryption section 100 using the common key is then transmitted to circuit switched network 22 through trunk 113 on the selected route of switch 110a.

Referring to FIG. 6, there is shown a preferred embodiment of encryption section 100, which encrypts outputs of analogue subscriber circuit 114 and digital subscriber circuit 115 and decrypts an output of trunk 113 in the opposite way.

In encryption section 100 shown in FIG. 6, terminal interface section 143 includes terminal interface circuit 143a and multiplexing/demultiplexing circuit 143b. Interfacing function to the analogue subscriber terminal 114 and the digital subscriber terminals 115 is carried out for data transfer through switch 110a.

Transmission line interface section 144 includes transmission line interface circuit 144a and multiplexing/demultiplexing circuit 144b, having interfacing

function with trunk 113 to transfer data through switch 110a.

Input/output section 145 provides an interface function between central processing circuit 120 of switching processing subsystem 111 in switching equipment 10 and control section 142. Encryption section 100 persistently maintains the public key (c) of central management & control equipment 20 and the private key (a) of the switching equipment (here, switching equipment 10) in key management section 141. As already illustrated in FIG. 1 to FIG. 3, the private key (a) is used for the reception of the public key (b) of the called switching equipment (for example, switching equipment 11) and the common key (a-b) for encrypting/decrypting main signal. (i.e. message information etc.) The reception is carried out on call-by-call basis from central management & control equipment 20.

When a call occurs from an originating party, switching equipment 10 automatically shifts the communication mode to perform secure communication. Alternatively, it may also be possible an originating party intentionally requests secure communication by adding a distinctive number specified for the secure service prior to the originating number.

In this case, detecting a distinctive number (a specified number for the secure service) in dialed information, switching equipment 10 recognizes the request for secure service in D-channel control circuit 130 and in supervisory circuit 131 (refer to FIG. 5). Accordingly, the secure service is started under the control of central processing circuit 120 in switching equipment 10.

When the secure communication mode begins, the control is started by control section 142 of encryption section 100 and central processing circuit 120 of switching equipment 10. In switching equipment 10, the called dial number and the user identification number are encrypted in center office key transfer control circuit 142c of control section 142. This is carried out according to the information of secure communication mode sent from central processing circuit 120, using the public key (c) of the center office. Then, central processing circuit 120 transmits the encrypted called number and user identification number to central management & control equipment 20, through common signaling channel network 21.

Central management & control equipment 20 decrypts the encrypted data sent from switching equipment 10 using the private key (c). Thus, the called number and the user identification number are recognized. Then, by retrieving database 201 (refer to FIG. 2) using the called number and the user identification number, the public key (b) of the switching equipment in which the destination terminal is connected (e.g. switching equipment 11) is obtained. Then, central management & control equipment 20 generates the common key (a-b) to encrypt the message actually being communicated between switching equipment 10 and switching equipment 11.

Using the public key (a) of switching equipment 10, central management & control equipment 20 further encrypts the common key (a-b) generated above and the public key (b) for communicating with switching equipment 11, to transmit to

switching equipment 10.

Switching equipment 10 decrypts the encrypted data received from central management & control equipment 20 in center key transfer control circuit 142c using the private key (a) of switching equipment 10. Accordingly, the public key (b) of switching equipment 11 and the common key (a-b) for the use of encrypting messages are obtained.

Switching equipment 10 selects a route in the switch via the switch control circuit by the control of central processing circuit 120, and performs connection processing in accordance with the called dial number. Meanwhile, upon completion of the connection, switching equipment 11 is shifted to the secure communication mode. At this point of time, encryption section 100 of switching equipment 10 and the encryption section of switching equipment 11 are connected through common channel signaling network 21.

When the connection is completed, the common key (a-b) is encrypted in common key control section 142b of encryption section 100 in switching equipment 10, using the public key (b) of switching equipment 11 already indicated from central management & control equipment 20. The encrypted common key (a-b) is then transmitted to the encryption section of switching equipment 11 by common key transfer circuit 140a in encryption processing section 140.

The encryption section of switching equipment 11 decrypts the received data using the private key (b) to regenerate the common key (a-b). At this point of time, sharing of the key for

secure communication, i.e. the key (a-b), is achieved between either of the switching equipment (actually between the encryption sections in each switching equipment) which respectively accommodates the related terminal.

When the common key is prepared in the encryption section of switching equipment 11, the confirmation information is transmitted back to encryption section 100 of switching equipment 10.

However, it may also be possible to send an inserted announce message to the related terminals so as to indicate the secure communication processing is in progress. During this procedure, the current state may be confirmed between central control circuit 142a in control section 142 and central processing circuit 120 in switching processing subsystem 111.

At the time the synchronization is completed between the encryption sections of switching equipment 10 and 11, the secure message communication is started. In encryption section 140 of switching equipment 10, the common key (a-b) shared with the encryption section of switching equipment 11 is transmitted to encryption processing section 140 from key management section 141 of encryption section 100. Encryptor 140b of encryption processing section 140 performs encryption using aforementioned common key (a-b) by means of the encryption scheme such as DES Triple DES, and so on. The encrypted message is transmitted to circuit switched network 22 through transmission line interface section 144.

In the encryption section (more precisely, in a decryptor

of the encryption processing section) of switching equipment 11, decryptor 140c decrypts the encrypted message already received using the common key (a-b). The above procedure is a reverse performed by encryptor 140b in switching equipment 10. The decrypted message is forwarded to the terminal. A message sent from switching equipment 11 is encrypted using the common key (a-b) similar to the procedure performed in switching equipment 10, and is transmitted to switching equipment 10.

On completion of the call, control section 142 of encryption section 100 indicates key management section 141 to discard both of the public key (b) and the common key (a-b), and the discard processing is executed accordingly.

Furthermore, the modification of the database in key management section 141 may be possible by transferring the public key (c) of central management & control equipment 20 and the private key (a) of the switching equipment. This is similar procedure to the aforementioned transmission/reception procedure to/from central management & control equipment 20. Use of the modification procedure produces not only easy key management but also enhanced confidentiality in the system.

FIG. 7 illustrates another preferred embodiment of the present invention. In order to improve the confidentiality, encryption and decryption are preferably carried out near to an originating point of information. From this viewpoint, it may be possible to provide security equipment in each terminal, as shown in FIG. 7.

Namely, as shown briefly in FIG. 7, a portion of the function

in encryption section 100 illustrated in FIG. 6 may be provided in the individual terminal 300. In FIG. 7, the encryption/decryption function of terminal 300 is controlled by control section 301.

Terminal 300 provides a register for a public key 303 of the own terminal and a register for a private key 302 corresponding to public key 303. Using private key 302, common key 304 is regenerated by decrypting the encrypted data transmitted from central management & control equipment 20 in a center office.

Therefore, it is possible to encrypt a message to be forwarded to the destination terminal in encryptor 305 using the regenerated common key 304, and to transmit to switching equipment 10 where terminal 300 is connected.

In the embodiment illustrated in FIG. 7, the function of encryption section 100 in switching equipment 10 may be simplified. That is; to encrypt a destination terminal dial number and a user identification number of switching equipment 10; then to inform central management & control equipment 20. This brings about simplified configuration of encryption section 100.

In accordance with the embodiment, the present invention enables to perform secure communication facility on call-by-call basis without necessitating key management in subscribers' premises. The key may be altered (compulsively) each time of secure communication. Unified key management performed by a center office enables to improve both

maintainability and secrecy. In addition, keys for transferring data between a center office and a plurality of switching equipment in a network may be changed when desired, because a common channel signaling network is used as communication path.

According to the present invention, a private network can be constituted which enables secure communication facility not requiring users' intervention. This will bring not only enhanced security but also improved secure communication facility individually applicable to the predetermined users without requiring system modification. Because of the unified key management performed by the central management and control equipment, management object can be limited. Key modifications executable whenever desired improve the system security. In case of the system extension, centralized control by the central management and control equipment can be realized. In addition, the combination of the encryptor (the scrambling scheme) can be modified call by call.

Having described the invention in detail, it will be apparent that other modifications and variations are possible without departing from the scope of the invention defined in the claims.